UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/802,485	03/09/2001	Burton S. Kaliski JR.	RSA-052	5894

7590 06/17/2004

Eric L. Prahl, Esq.
HALE AND DORR LLP
60 State Street
Boston, MA 02109

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	**PAPER NUMBER**
2135	10

DATE MAILED: 06/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/802,485	KALISKI, BURTON S.
	Examiner	Art Unit
	Paula W Klimach	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claims 1, 21 is objected to because of the following informalities:

Claim reads "*receiving by a server from a client client information,*" should read "*receiving, by a server from a client, client information.*" Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claim 1-4, 9-11, 14-16, 21-22, 26-27, 31, 33, 37-38, 41, and 42 are rejected under 35 U.S.C. 102(a) as being anticipated by Stallings.

In reference to claims 1, 21, 31, 37, 38, and 42, Stallings teaches a method for accessing encrypted data by a client, the method comprising the steps of: receiving, by a server from a client, client information derived from a first secret (page 143 paragraph 3 message 1). The nonce described by Stallings is sent from the user A and should be difficult for an opponent to guess; the value may be a random number derived from a seed that is secret. Stallings teaches the client information is derived such that the server cannot feasibly determine, find out by means of calculation or by investigation, the first secret; as a result the nonce is sent to the key distribution center (server). The key distribution center then sends the user A intermediate data derived from the nonce sent by the user A and therefore the intermediate data derived responsive to at least the received client information. The server secret that is included is the key shared by

the server and the user B, K_b. The value K_b is shared by the key distribution center (server) the value is created such that an outside device cannot determine it (page 144 paragraph 1 message 2). The user B using message 3 then authenticates the user A. The message 2 contains the request and the nonce of message 1. The user A is authenticated because it knows the value shared by the user B and the key distribution center (server). User B, the authentication device, contains encrypted secrets such as the nonce N_2. The user B would not divulge the secrets without the key K_b because K_b informs the user B that the session key comes from the key distribution center (server). The encrypted secrets such as the nonce are decrypted using the session key K_s that was received in the intermediate data.

In reference to claims 2, 22, 33 and 41, wherein the third secret is derived from the intermediate data by use of one of a key derivation function and a hash function. The key derivation function used in the method disclosed by Stallings is the decryption function (Fig. 5.9).

In reference to claim 3, wherein the third secret is the intermediate data. The third secret (K_s) is the intermediate data because the third secret is used to decrypt the secret and K_s is used to decrypt the secret such as the nonce N_2 (Fig. 5.9).

In reference to claim 4, wherein the first secret comprises at least one of a PIN, a password, and biometric information. The nonce described by Stalling is in the form of a unique identifier which corresponds to a password or PIN or biometric (page 143 paragraph 3 message 1).

In reference to claim 9, wherein the authenticating step comprises authenticating the client based on at least one of a PIN, a password, and biometric information. The step 3 includes

sending ID information of the user A (page 144). PIN, password, and biometric information correspond to ID information.

In reference to claims 10 and 26, wherein the authenticating step comprises authenticating the client based on a secret other than the first secret. The user A uses information, to authenticate itself with user B, that does not include the first information sent to the key distribution center (Fig. 5.9).

In reference to claims 11 and 27, wherein the authenticating step comprises using a secret derived from the intermediate data. The authenticating step uses the session key K_s which is derived form the message 2 (Fig. 5.9).

In reference to claim 14, wherein the encrypted secrets comprise a private key of a public/private key pair used for asymmetric cryptography. Stalling discloses the Nonce as being a random number. The value sent by the user B is a Nonce, N_2. Stalling further discloses the user of a random number in calculating the private key for the public key pair (page 177-178).

In reference to claim 15, wherein the encrypted secrets comprise a signature key used for creating a digital signature. Stalling further discloses the using private and public key for the generation of a digital signature (pages 312-313).

In reference to claim 16, wherein the authenticating step comprises authenticating the client based on a secret other than the first secret, so that the user provides different information to access the device and access the signature key (Fig. 5.9). Stalling discloses a method wherein the user A provides the user B information to authenticate itself that is different from the information presented to the key distribution center.

In reference to claim 39, further comprising the step of transmitting to the first server by the network server verification that the user has authenticated successfully. The response of the N_2 is a confirmation of the authentication of user A since user B would not be able to communicate N_2 if user A did not authenticate.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim17, 32, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings.

In reference to claim 17, The method of claim 1 wherein the encrypted secrets comprise a secret key used for symmetric cryptography.

Stallings does not disclose the encrypted secrets comprising of a secret key used for symmetric cryptography.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to insert a secret key instead of the Nonce as in part 4 Fig. 5.9 in the system of Stallings. One of ordinary skill in the art would have been motivated to do this because the user

A and the user B are already able to communicate in a secure manner using the key K_s, however the session key needs to be replenished often.

In reference to claims 32 and 40, wherein the network server is a web server and wherein the client is a web browser.

Stallings does not disclose the network server as a web server and the client is a web browser

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to make the user B a web server and the user A a web browser in the system of Stallings. One of ordinary skill in the art would have been motivated to do this because the user A and B were placeholders for devices that need authentication which is necessary for the Internet and therefore for network browsers that require access to servers.

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Schneier.

In reference to claim 8, wherein the authenticating step comprises authenticating the client based on a time-dependent code. Stallings does not expressly disclose the client authenticating based on a time-dependent code.

Schneier discloses the use of the timestamp during authentication (page 61). The information used during authentication is then time-dependent.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a time stamp during authentication as in Schneier in the system disclosed by

Stallings. One of ordinary skill in the art would have been motivated to do this because the time stamp would prevent replay attacks.

Claims 5-7, 18, 23-25, 29, and 34-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Spellman et al (5,638,445).

In reference to claims 5 and 23, Stallings does not disclose a blind function evaluation protocol used to derive the intermediate data from the secret data.

Spelman discloses a merchant device deriving an intermediate message from a secret message sent by the consumer. The merchant device uses blind encryption to determine the intermediate data (Fig. 1 in combination with column 6 lines 15-30).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to blind the secret data as disclosed by Spelman in the system disclosed Spallings. One of ordinary skill in the art would have been motivated to do this because it would facilitate communication between devices in the case that the keys have not been exchanged yet.

In reference to claims 6, 24, 34, and 35, wherein the security of the blind function evaluation protocol is based on the problem of extracting roots modulo a composite.

Stallings does not disclose the user of a blind function.

Spelman discloses the user of a blind encryption function wherein the evaluation protocol is based on the problem of extracting roots modulo a composite (column 6 lines 31-44).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to blind the secret data as disclosed by Spelman in the system disclosed Spallings.

One of ordinary skill in the art would have been motivated to do this because it would facilitate communication between devices in the case that the keys have not been exchanged yet.

In reference to claims 7 and 25, wherein the security of the blind function evaluation protocol uses discrete logarithms.

Stallings does not disclose the user of a blind function.

Spelman discloses the user of a blind encryption function wherein the evaluation protocol uses the discrete logarithm problem (column 6 lines 31-44).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to blind the secret data as disclosed by Spelman in the system disclosed Spallings. One of ordinary skill in the art would have been motivated to do this because it would facilitate communication between devices in the case that the keys have not been exchanged yet.

In reference to claim 18, wherein the encrypted secrets comprise at least one unit of digital currency.

Stallings does not disclose the encrypted secrets comprising at least one unit of digital currency.

Spelman discloses the data being sent from a merchant to a merchant acquirer, therefore the information includes digital currency with visa information (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send digital currency as suggested by Spelman in the system disclosed Spallings. One of ordinary skill in the art would have been motivated to do this because communication of currency requires enhanced security to prevent theft.

In reference to claim 29, wherein the encrypted secret comprises at least one secret chosen from the set of a private key of a public/private key pair used for asymmetric cryptography, a signature key used for creating a digital signature, a secret key used for symmetric cryptography, and at least one unit of digital currency.

Stalling further discloses the using private and public key for the generation of a digital signature (pages 312-313). However Stalling does not disclose symmetric cryptography of digital currency

Spelman discloses the data being sent from a merchant to a merchant acquirer, therefore the information includes digital currency with visa information (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send digital currency as suggested by Spelman in the system disclosed Spallings. One of ordinary skill in the art would have been motivated to do this because communication of currency requires enhanced security to prevent theft.

In reference to claim 36, wherein the encrypted secrets comprise encrypted personal information associated with a user of the client.

Stalling does not expressly disclose the encryption of personal information associated with the user of the client.

Spelman discloses the encryption of visa information that is personal information associated with a user of the client (consumer; Fig. 2D).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt personal information as suggested by Spelman in the system disclosed

Spallings. One of ordinary skill in the art would have been motivated to do this because communication of currency requires enhanced security to prevent theft.

Claims 12-13, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Richard et al (5,922,074).

In reference to claims 12 and 28, wherein the device comprises at least one of a file server, a directory server, a key server, a PDA, a mobile telephone, a smart card, and a desktop computer.

Stallings does not expressly disclose the device comprising at least one of a file server, a directory server, a key server, a PDA, mobile telephone, a smart card, and a desktop computer.

Richard discloses a system that includes a directory server from which the client authenticates to gain access (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the client to a directory server as in Richard in the system of Stalling. One of ordinary skill in the art would have been motivated to do this because the directory includes sensitive information that requires increased security.

In reference to claim 13, wherein the device comprises at least one secure data store, the device-requiring authentication before allowing the client access to the data store.

Although Stallings discloses a system wherein the device requires authentication before allowing the client access to the data, Stallings does not expressly discloses as system wherein the device comprises at least one secure data store.

Richard discloses a system wherein the client authenticates itself to a server that stores information or services (column 6 lines 21-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the client to a server that stores information or services as in Richard in the system of Stalling. One of ordinary skill in the art would have been motivated to do this because the directory includes sensitive information that requires increased security.

Claims 19-20 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Brunsting et al (6,505,164).

In reference to claims 19 and 30, further comprising the step of verifying that the client has not exceeded a predetermined number of unsuccessful ,attempts to obtain the intermediate data.

Stalling does not disclose a system that maintains a count of the number of unsuccessful attempt to authenticate a system.

Brunsting discloses a system that maintains a count of the number of unsuccessful attempts at accessing account information (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a count of the number of unsuccessful attempts as in Brunsting in the system of Stalling. One of ordinary skill in the art would have been motivated to do this because it would increase security by monitoring the activity that may be malicious.

In reference to claim 20, wherein the verifying step further comprises: transmitting a challenge code to the client; and receiving the result of a cryptographic operation using the challenge code as an input and using a cryptographic key derived from the encrypted secret. Stalling discloses the user B sending the user A a nonce N_2 as a challenge that user A answers as input to a function that uses the K_s as a key (parts 4 and 5 fig. 5.9).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

PWK
Thursday, June 10, 2004